PAUL, HASTINGS, JANOFSKY & WALKER LLP
BRADFORD K. NEWMAN (SB# 178902)
SHANNON S. SEVEY (SB# 229319)
PATRICK M. SHERMAN (SB# 229959)
Five Palo Alto Square
Sixth Floor
Palo Alto, CA 94306-2155
Telephone: (650) 320-1800
Facsimile: (650) 320-1900

Attorneys for Plaintiff
ArcSoft Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

ARCSOFT, INC.,

Plaintiff,

vs.

PAUL FRIEDMAN, and DOES 1 through 50,

Defendants.

CASE NO. C 07-03512 SC

DECLARATION OF LEE CURTIS IN SUPPORT OF ARCSOFT INC.'S APPLICATION FOR TEMPORARY RESTRAINING ORDER

Date: July 6, 2007
Time: 9:30 a.m.
Dept: Courtroom 1, 17th Floor
Bef: The Hon. Samuel Conti

I, LEE CURTIS, hereby declare as follows:

1. I am the Managing Director of Aon Consulting ("Aon") and specialize in investigations concerning network intrusions, computer forensic analysis, trade secret theft, and intellectual property matters.

Background

2. I have more than 40 years of combined experience in law enforcement, high tech investigations, and security technology consulting. I served in law enforcement for more than 30 years, performing both Federal and State criminal investigations, and have 12 years of experience in the field of computer forensics. I was certified as a Computer Investigative Specialist in 1996. I have qualified as an expert in the area of high tech investigations and computer forensics in California Superior Court and the United States District Court.

3. Prior to joining Aon Consulting, I served in the field of law enforcement for more than 30 years, performing both Federal and State criminal investigations. I retired from the Internal Revenue Service in 1998 as a Special Agent with the Criminal Investigation Division. In that role, I served as a Criminal Investigator, Group Manager, and Computer Investigative Specialist on extensive financial investigations, involving forensic accounting, computer evidence recovery, and data analysis. My responsibilities included investigating and providing oversight for domestic and international investigations of federal criminal violations including tax evasion, money laundering, illegal currency transactions, perjury, conspiracy, bank fraud, and bankruptcy. After retiring from the Internal Revenue Service, I served as a criminal investigator in the High Tech and White-Collar Crime Unit of the Santa Clara County District Attorney's office, from 1998 through 2000 where I conducted computer forensic examinations for the purpose of criminal prosecution.

4. After leaving public service in 2000, I joined the private sector and became a Director for Kroll Associates, Inc., managing their computer forensics unit. In early 2002, I left Kroll and joined KPMG, in its Forensics Practice Division, handling all matters for KPMG in the Western United States. I subsequently accepted a Senior Managing Director position in December 2003, for CoreFacts, Inc., a national firm specializing in computer forensic recovery

and private investigation. In February 2005, I returned to Kroll as the Director of Investigative & Security Technology Consulting. In February 2006, I accepted the current position I hold with Aon Consulting.

5. I have participated in and/or supervised the forensic examination of over one thousand computers. I have attended computer forensic training courses at the National Consortium for Justice Information and Statistics SEARCH School in Northern California and the Federal Law Enforcement training center in Brunswick, Georgia. I received advanced forensics training at North Texas University. I continue to receive training through the High Tech Criminal Investigators Association (HTCIA) and specialized training provided by computer forensic software manufacturers including Guidance Software. I was certified as a Computer Investigative Specialist, in 1996. I have taught on the subject of high tech investigations to both federal and local law enforcement officers, including teaching computer forensics at the Federal Law Enforcement training center. I presently teach forensics for Peace Officers Standards and Training (POST) for the California Department of Justice.

Technology Used For Forensic Examination

6. The method Aon uses to copy the contents of a computer ensures the integrity of all existing data contained therein and does not modify in any way the existing data contained on the hard drive. Using a software program called "EnCase," Aon creates an image file (often referred to as a mirror image) of the evidence hard drive as follows: (1) the hard drive is attached to an analysis computer via a hardware write blocking device which ensures the data on the subject computer is not changed; (2) Aon creates a complete forensic image copy or "exact snapshot" of a targeted piece of computer media, such as a hard drive. This forensic image is a complete sector-by-sector copy of all data contained on the target media and thus all information, including available information from deleted files, is included in the forensic image created. Analysis can be performed on the image file directly or the image can be used to create a duplicate clone hard drive which can be further analyzed. The image file and the original evidence hard drive remain completely unaltered from the time Aon acquires it.

7. EnCase is a standard, commercially available software program that is

specifically designed as a tool for computer forensic investigations. It is a fully integrated tool, meaning it performs all essential functions of a computer forensic investigation, including the imaging of a target drive, the generation of an MD5 hash value of the evidentiary forensic image, and facilitates much of the analysis of the subject evidence. The software allows for a completely non-invasive investigation in order to view all information on a computer drive, whether it is in the form of a deleted file, a non-deleted file, file fragments, and even temporary buffer files. EnCase is widely used in the computer forensics industry and, in my experience, it is the tool of choice of the majority of computer forensic investigators in law enforcement. It is the primary computer forensic tool used by several federal agencies, including the U.S. Customs agency and the United States Secret Service.

8. Aon's forensic investigation methods are court-proven. I have testified in numerous criminal and civil cases as an expert in computer forensic analysis and to my knowledge, no court has ever faulted the EnCase software and forensic methodology Aon uses. Aon's methodology ensures the integrity of the evidence and the chain of custody.

Electronic Data, Generally

9. Computer evidence resides mostly on magnetic media, usually hard drives, diskettes, or tape. Magnetic media of these kinds are designed to retain their information for long periods, typically many years, without change, unless their contents are overwritten with new data. Even data that someone generally deletes in the course of normal operations leaves an imprint on the medium where it resided after deletion, until such time as someone overwrites the space that data occupied with new information, or the data is deliberately destroyed via wiping and intentional overwriting.

10. Files on a disk or tape will remain intact until they are altered, deleted, or overwritten. Until someone overwrites a file, it tends to remain in the exact same condition since the time at which it was created or last changed. Once a file has been deleted, the data is at continuing risk of being overwritten. Once a file is overwritten, it is effectively lost forever.

Work Performed For ArcSoft Inc.

11. Aon was retained to provide computer forensic consulting services for ArcSoft,

Inc. Aon was asked to preview and, if possible, image the Sony laptop computer it was informed Paul Friedman returned to ArcSoft's Corporate Counsel, Victor Chen, on June 27, 2007 ("Laptop"). Aon was informed that Friedman had been terminated on June 26, 2007, and had immediately taken the Laptop with him when he exited ArcSoft and that ArcSoft did not recover the Laptop until the afternoon of the following day.

12. Aon was asked to do the following: (1) preview the hard drive in the Laptop with a forensic write-blocker; (2) forensically image the contents of the hard drive to the extent that recoverable data still existed; (3) create data spreadsheets that included the file and folder names, types, creation dates and "last modified" dates files from files, folders and file data that had been deleted from the Laptop; (4) restore, as much as possible, all files, folders and file data that was not deleted but still existed in readable form.

13. I supervised the work that Aon performed for ArcSoft on this matter.

14. On or about June 28, 2007 at approximately 9:30 a.m., at the Fremont offices of ArcSoft, Aon received from ArcSoft a Sony Vaio laptop computer, Serial Number 281326303201143, which contained a hard drive, Serial Number 720TA1YZIE. I am informed that this computer is the Laptop Friedman had been issued by ArcSoft, took upon the termination of his employment on June 26, 2007, that was recovered by ArcSoft from Friedman on June 27, 2007.

15. Chen informed Aon that, upon receiving the Laptop and observing Friedman as he attempted to boot up the computer, Chen saw the words "disk error" appear on the screen of the Laptop. Based on this information, Aon became concerned that the Laptop's Microsoft Windows program was not operating properly.

16. Based on the information provided, Aon concluded that it should begin its work by attempting to "preview" the hard drive using the EnCase software program. "Previewing" is performed by first attaching a write blocker to the hard drive at issue (which prevents the hard drive from being altered in any manner), and then activating the "preview" mode in EnCase to review the contents of the hard drive.

17. Aon was unable to preview any content on the hard drive. When Aon attempted to review the hard drive of the Laptop, a single pattern of "..............................." appeared across all sectors of the hard drive. Viewed in hex mode (which is a binary method of reflecting data), every byte in every sector of the Laptop's hard drive contained the value of hex 00, which is consistent with a hard drive being erased, or "zeroed out" (as it is also known). This information indicates that the hard drive of the Laptop had no data, no partition, no master file table, and no information on the hard drive. More specifically, this information indicates that, to the extent the hard drive in the Laptop contained an operating system or any data in the past, it had been overwritten.

18. Aon verified this result by performing its methodology again. The second attempt to Preview the hard drive of the Laptop produced the same result.

19. Based on the repeated "..............................." pattern and the lack of any data, partition, master file table, or other information, Aon concluded that a wiping program had been used to erase the entire contents of the hard drive of the Laptop.

20. I am aware of no other action, other than using a program designed to wipe the entire contents of a hard drive, that a computer user could perform to cause the "..............................." pattern (or hex value 00) to appear throughout the entire hard drive of a computer.

21. I am informed and understand that Friedman has a Bachelor of Administration degree in Computer Science. Based on my experience in the computer forensics industry, it is my opinion that a person with an educational background similar to that of Friedman would have the knowledge and capability necessary to use an erasing program to wipe the data, partition, master file table, and all other information from the hard drive of a computer.

Evidence Preservation

22. Because it is relatively easy to permanently delete a document from a hard drive, in cases where there is some reason to be concerned that the subjects of the investigation may delete all or some of the computer files that contain evidence of wrongdoing, in my professional opinion, it is important to gain early and immediate discovery into all computers and electronic

storage devices that the subjects currently have access to so as to take reasonable measures to prevent permanent destruction of evidence.

23. Given the facts known to me in this case, including the forensic examination of the evidence residing on the computer, it is my opinion that there is a reasonable possibility that valuable information may be obtained from the examination of the user's home computers, Internet email accounts, and any other computer or electronic storage device the user accessed between October 15, 2006 and the present, including those computers and storage devices to which he currently has access. This would include both personally owned computers and computers assigned to the user by his current employer.

24. In this particular case, where there was a clear intent to improperly retain the computer, to refuse a police officer's request to return it, and then to return it after it had been wiped, there is a probability that before it was wiped, the subject surreptitiously copied the Company's confidential and proprietary information. Accordingly, I believe it is imperative that Aon be given immediate access to the subject's current computer(s) and electronic storage devices to preserve whatever evidence may have been transferred to these devices prior to the subject wiping the computer. Intentional wiping is primarily used to destroy evidence of accessing, copying and removing data from a computer. It is important to preserve where the data was moved to and the data itself.

25. Concerns over the protection of the privacy of the computer owner are easily addressed. I have been retained in a number of cases of civil litigation with similar concerns. The remedy is a protective order prepared by the attorneys involved and approved by the court, stating that Aon will conduct an examination in such a way as to provide the maximum possible protection to the privacy of the computer owner. Material on the computer that is unrelated to the litigation will not be disclosed to any party. Aon alone will maintain the image copy of the hard drive and will not disclose its contents to any person without the consent of the owner, his attorney or an order from the court. All information extracted from the computer to be disclosed as part of this litigation will be approved for release by the owner and/or his attorney. Items discovered during the analysis, but precluded from disclosure by claims of privilege, will be

documented in a privilege log. Disputes over the release of particular information will be decided by the presiding court. My participation in the matter would be similar to that of a special master. The computer(s) to be examined should be removed from service immediately. At a minimum, removal from service would constitute being turned off and not turned back on for any reason until after a forensic examination. Ideally the computer should also be placed in the custody of a trusted neutral party. Creating an image file from a hard drive usually takes between one hour to six hours per computer depending on the type of computer and the size of the hard drive in question. This process is easily done on site, often at the offices of one of the attorneys involved. After the computer(s) have been examined and their hard drives imaged, at the discretion of the attorneys, they may be returned to their user and resume normal use.

I declare under penalty of perjury that the foregoing is true and correct, unless stated on belief. This Declaration was executed on July 2, 2007 in Palo Alto, California.

LEE CURTIS